



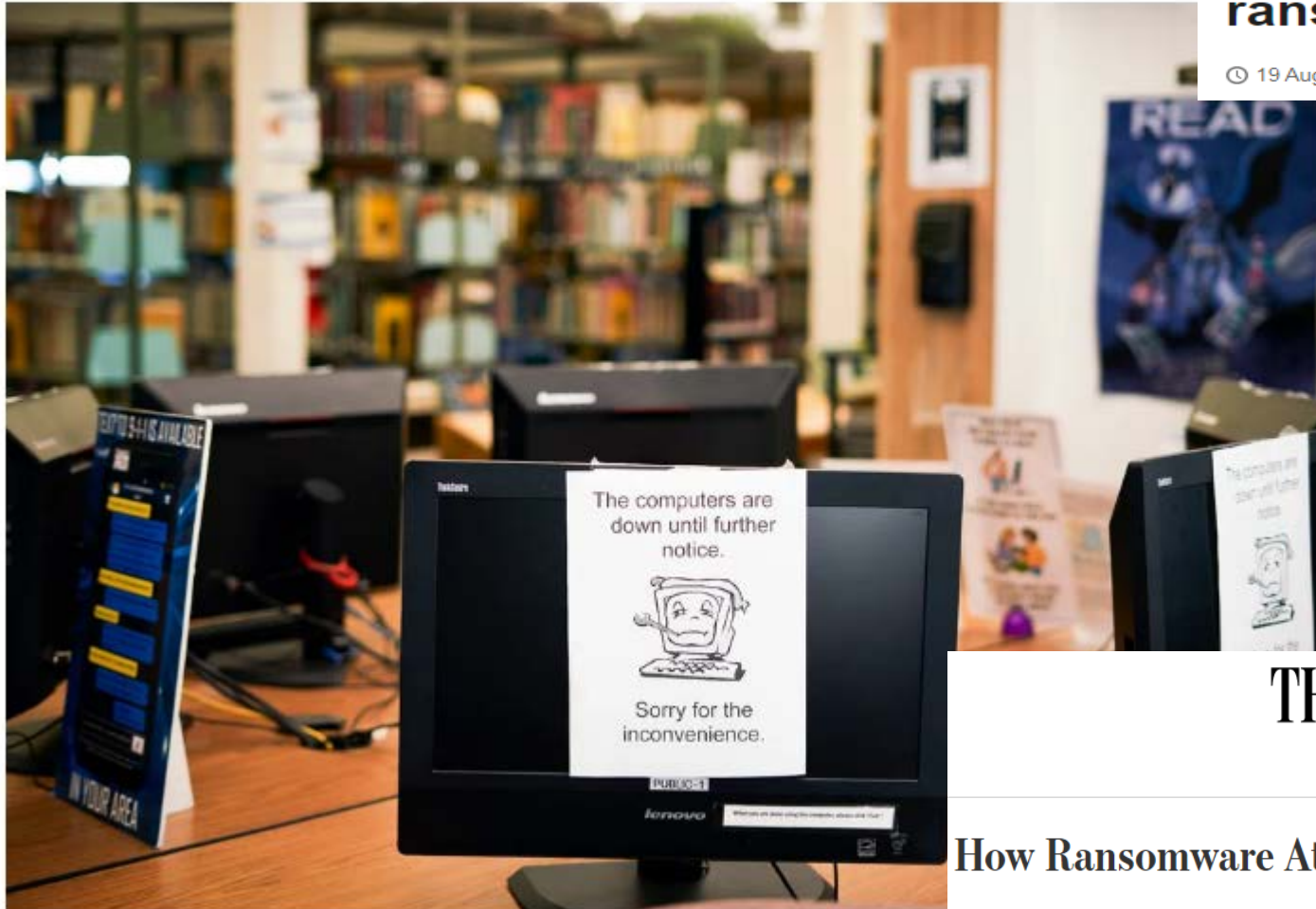
Cybersecurity Presentation

October 7, 2019

City of San Leandro City Council Meeting



Ransomware Attacks Are Testing Resolve of Cities Across America



Computers were shut down at the E.M. Gilliam Memorial Library following a ransomware attack in Wilmer, Tex. Cooper Neill for The New York Times

NEWS

Home

Video

World

US & Canada

UK

Business

Tech

Science

Stories

Ente

Technology

Texas government organisations hit by ransomware attack

19 August 2

CBS NEWS

NEWS

IMPEACHMENT INQUIRY

SHOWS

LIVE

Grid icon

Search icon

Ransomware attacks on the rise – and small towns are in the crosshairs



City of Baltimore

Subscribe

Start by searching
i.e. "How do I pay my parking ticket?"

Search

News

Online Payments

How Do I?

311 Services

Government

Events

Office of the Mayor

Connect

The City of Baltimore is currently unable to send or receive email. If you need assistance, please call the department you wish to contact.

[Click here](#) for information on Baltimore city services / contact numbers.

THE WALL STREET JOURNAL.

How Ransomware Attacks Are Forcing Big Payments From Cities, Counties

Who is Behind the Attacks?

ACTUAL LIST FROM FBI MOST WANTED

<https://www.fbi.gov/wanted/cyber>



OUTMODED MOVIE
STEREOTYPE



GOZNYM SUBJECTS



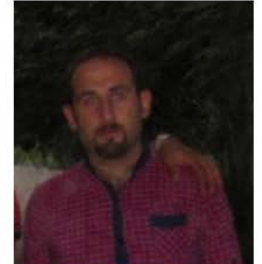
FUJIE WANG



IRGC-AFFILIATED CYBER
ACTORS



MOJTABA MASOUMPOUR



BEHZAD MESRI



HOSSEIN PARVAR



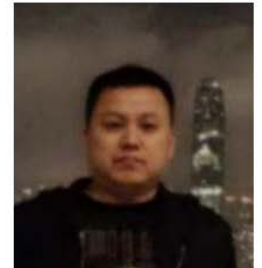
MOHAMAD PARYAR



APT 10 GROUP



ZHANG SHILONG



ZHU HUA



Why is the Public Sector Targeted?



**MISSION CRITICAL
OPERATIONS**

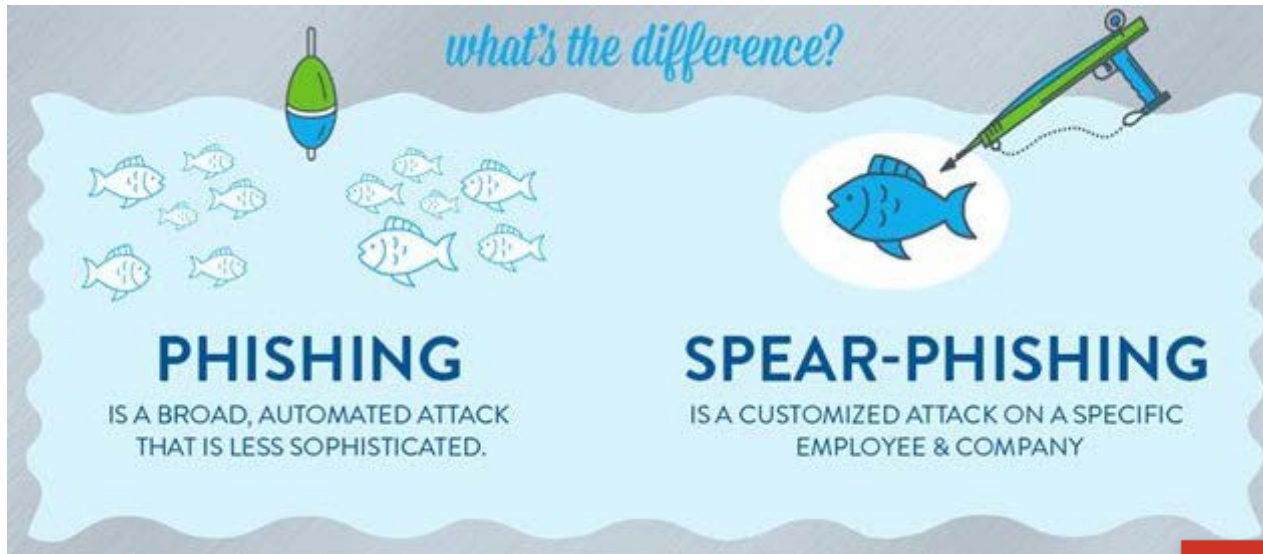


BUDGET/FUNDING



**LEGACY
INFRASTRUCTURE**

How Do Attacks Happen?

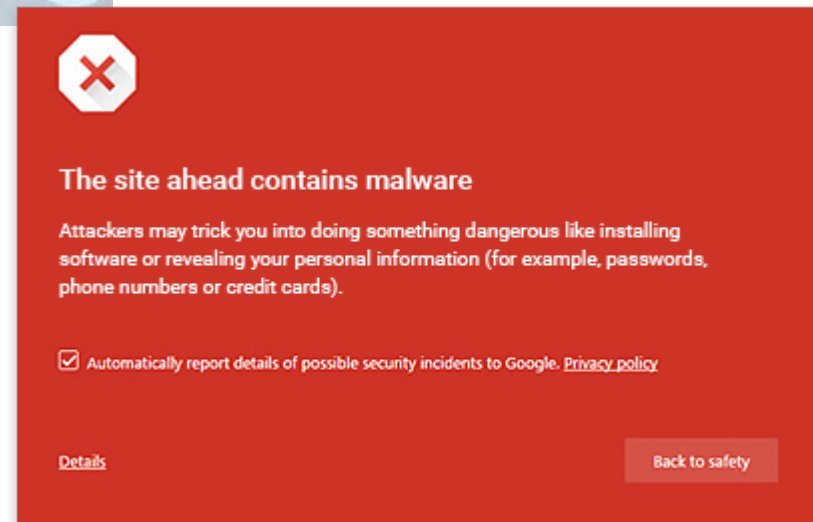


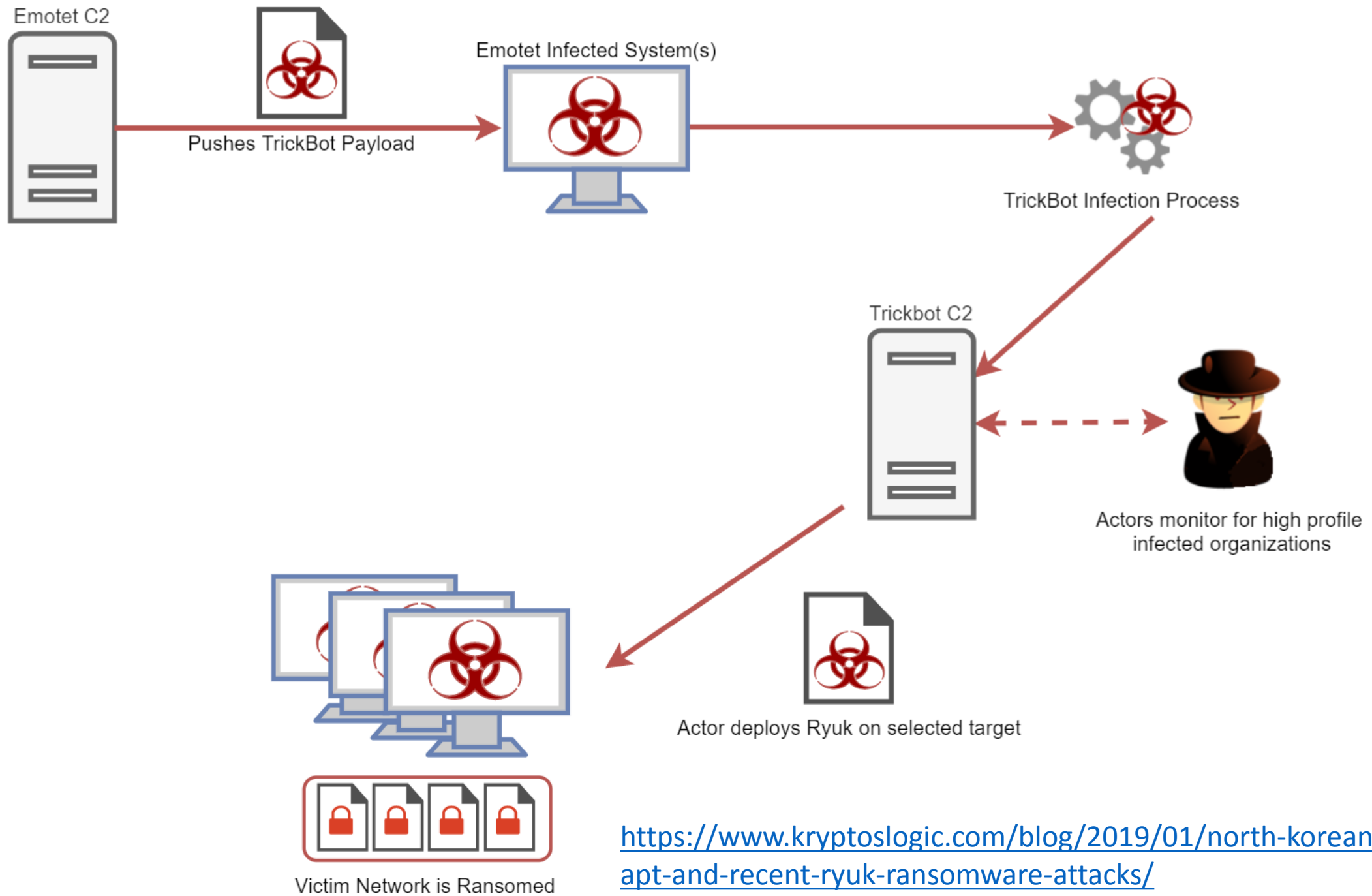
EMAIL

WEB

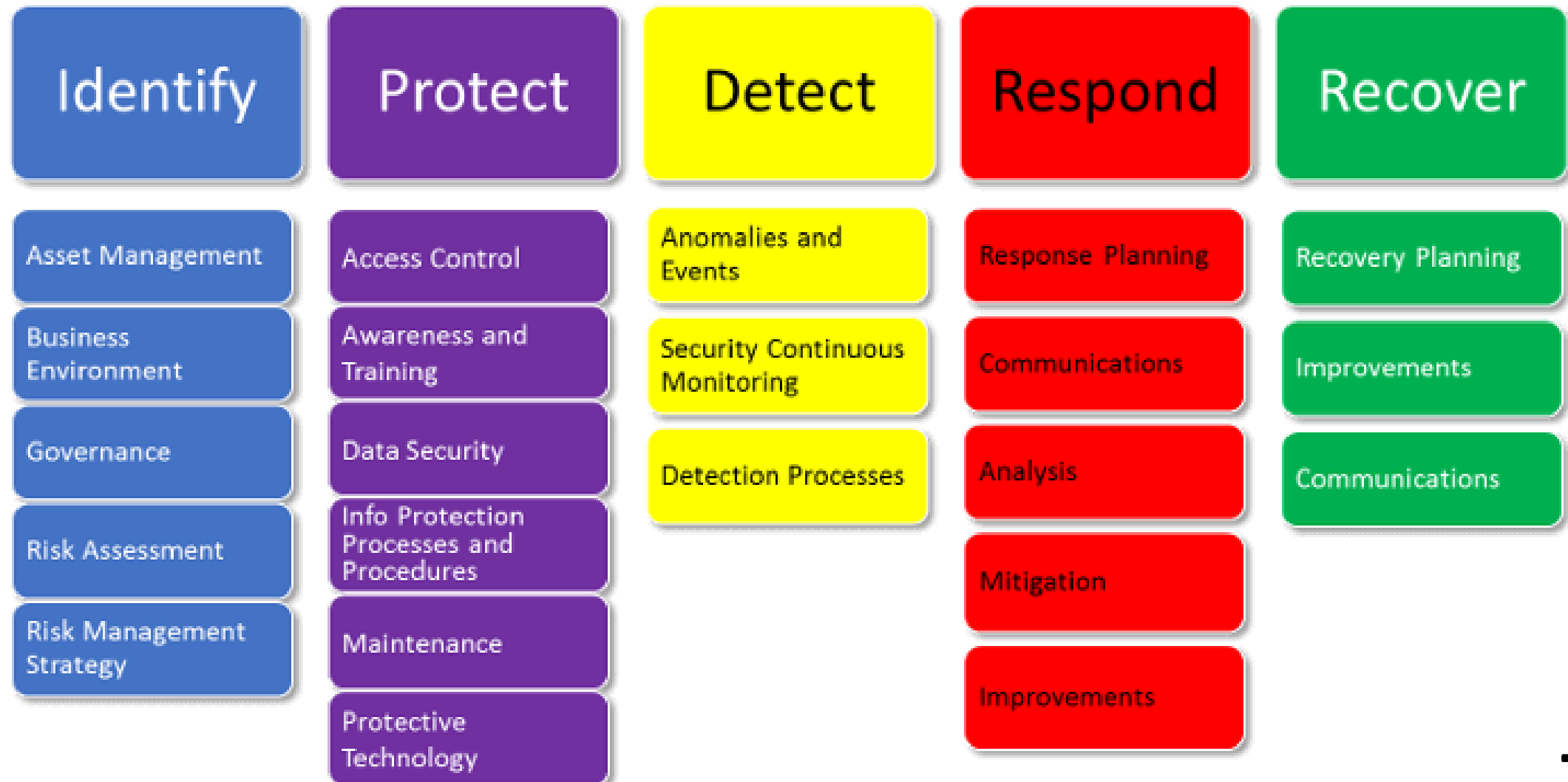


NETWORK



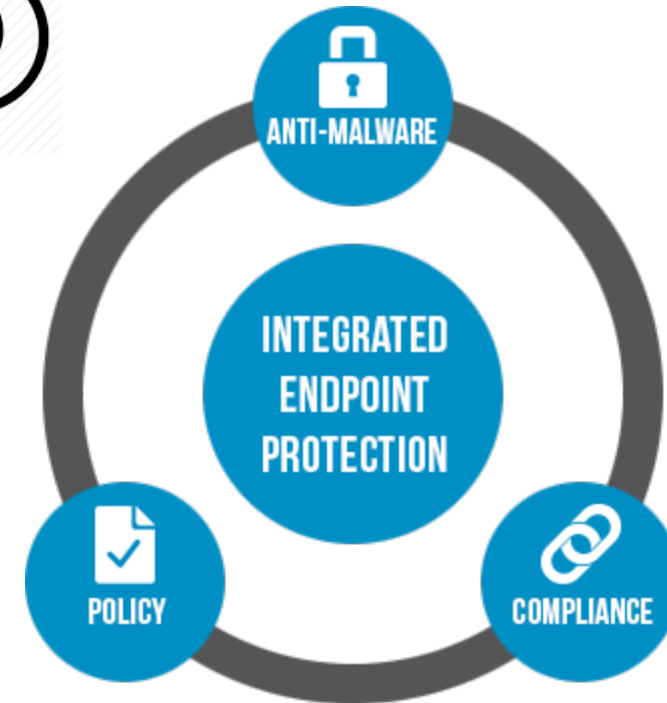


NIST Cyber Security Framework



What Have We Done So Far?

- Modernized Infrastructure
- ~60% of systems are Cloud-Hosted
- “Next Gen” Firewalls (IDS & IPS & Content Filtering)
- 365 Advanced Threat Protection (Links, Attachments)
- Endpoint Protection on City desktops/laptops
- Working with CryptoMove, Maze & Associates, and NCRIC





Still More To Do



Work with Maze on a Ransomware Assessment



Add't Endpoint Protection



User Awareness Training

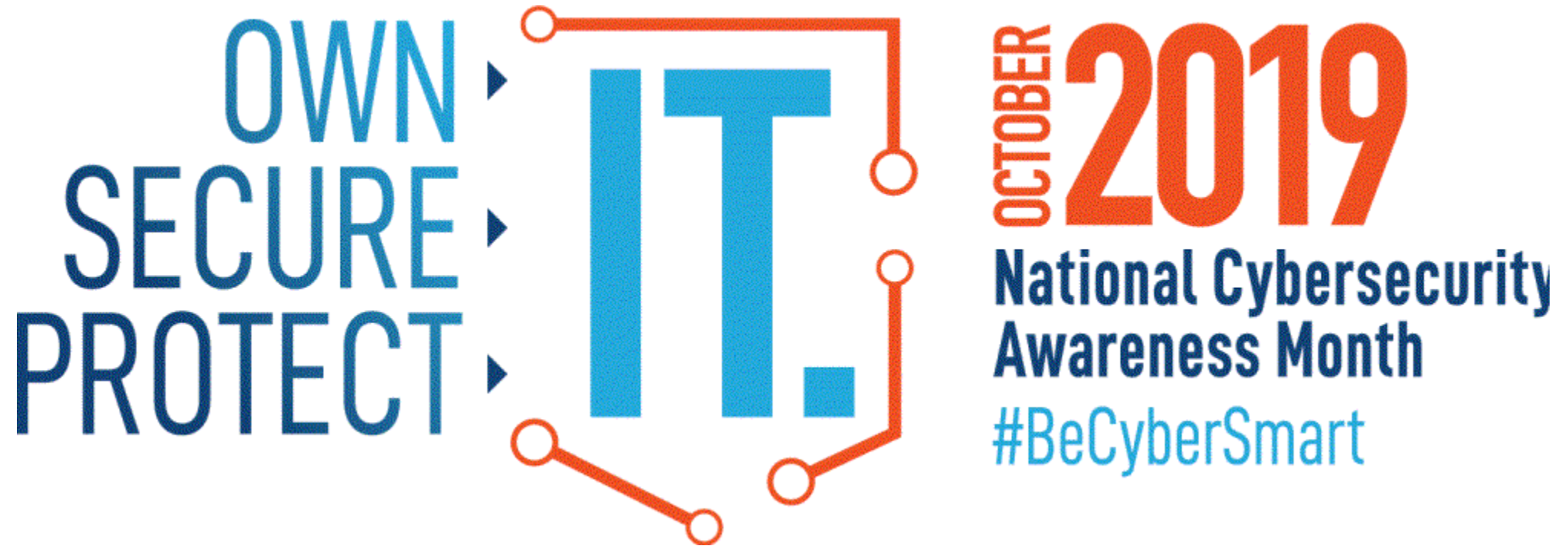


Replace Backup System + Build Disaster Recovery System



Regional Collaboration on Incident Response
(Nearby Cities, Counties, NCRIC, PD, EOC)

Cybersecurity Awareness Month 2019



→ <http://sanleandro.org/depts/it/cyberawareness/default.asp>